

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT
for the
Northern District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

A Microsoft 256 GB laptop, number 055196290353 and a)
SanDisk 400 GB micro-SD card, serial number)
2175YXHT12EN, which are located at FBI Albany, 200)
McCarty Ave, Albany NY 12209)

Case No. 1:23-mj-00053 (DJS)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

- 18 U.S.C. § 2251(a) and (e)
- 18 U.S.C. 2252A(a)(1)
- 18 U.S.C. § 2252A(a)(2)(A)
- 18 U.S.C. 2252A(a)(5)(b)

Offense Description

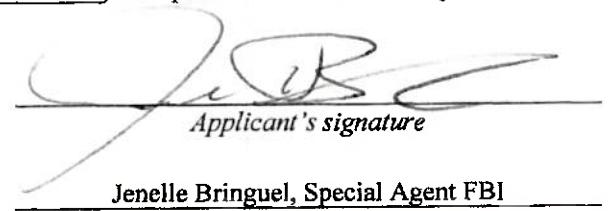
- Exploitation and attempted sexual exploitation of a child and Transportation of child pornography
- Distribution of child pornography
- Possession of child pornography

The application is based on these facts:

See attached affidavit

Continued on the attached sheet.

Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Jenelle Bringuel, Special Agent FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone (specify reliable electronic means).

Date: January 23, 2023City and state: Albany, NY


Judge's signature

Hon. Daniel L. Stewart, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jenelle C. Bringuel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— electronic devices — which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since 2012. While employed by the FBI, I have investigated federal criminal violations related to child sexual exploitation and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Microsoft 256 GB laptop, number 055196290353, and a SanDisk 400 GB micro-SD card, serial number 2175YXHT12EN, which was inserted into the laptop. (Hereinafter the laptop and SD card are referred to as the “Devices.”) The Device are currently located at FBI Albany, 200 McCarty Ave, Albany NY 12209.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On January 12, 2023, I was the affiant on a criminal complaint charging Trevor Metterhauser with attempted production of child pornography, in violation of 18 U.S.C. § 2251(a) and (e). A copy of the complaint and affidavit in support are attached as **Exhibit 1** and incorporated by reference here. In sum, Metterhauser traveled from his home in Pennsylvania to the Albany, New York area planning to have sex with a 10-year-old deaf child (who was fictitious), record his sexual abuse of the child, and sell the recording on the dark web.

7. During a *Mirandized* interview on January 12, 2023, Metterhauser consented to the search of the car he drove from Pennsylvania to New York. The FBI's initial consent search did not find the Devices because the car was extremely cluttered. During his interview, Metterhauser said that he had a laptop in his car, described the laptop's location within the car, and said that the laptop had child pornography files on it. Based on that information, investigators re-entered Metterhauser's car and retrieved the laptop, which upon subsequent visual examination was seen to have an SD card inserted into a data port. The complaint affidavit incorporated herein by reference also explains that Metterhauser admitted to traveling from Pennsylvania to the Ithaca, New York area in November 2022 where he participated in the creation of recordings depicting the sexual abuse of an approximately 4-year-old female child and to traveling from Pennsylvania to Texas in December 2022 where he participated in the creation of recordings depicting the sexual abuse of an approximately 2-year-old child.

8. Metterhauser also consented to a search of his cellular telephone. Investigators have identified several child pornography files on that device, including the following:¹

¹ These files are available for the Court's review upon request.

- a. A 9 minute 20 second video depicting an adult female performing oral sex on an approximately 4-6-year-old female (MD5 Hash 7c04a2d55cb2303122558db207aa594b);
- b. A 10-minute video depicting a naked adult female touching the vagina of a naked 4-6-year-old female while the child uses her hand to stimulate the erect penis of an adult male (MD5 Hash 097f71ddbba804b0a078bc185b5e05af);
- c. A 28 second video depicting an 8-10-year-old female rubbing her naked vagina, which is the focal point of the video (MD5 Hash 771e4a937116e4d5b8304565cf00e978).

9. The Devices are currently in the lawful possession of the FBI as described above. Therefore, while the FBI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

10. The Devices are currently in storage at the FBI Albany office, 200 McCarty Ave, Albany, NY 12209. In my training and experience, I know that the Devices have been stored in a way that their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

11. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives.

Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

b. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service

providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. Based on my training, experience, and research, I know that the Devices have capabilities that, together, allow them to serve as a digital camera, portable media player, tablet, and data storage device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. I also know from my training and experience that people use electronics like the Devices to communicate with others on social media applications, including to trade child pornography as discussed further below, and to plan trips like the one Metterhauser took from Pennsylvania to New York for the purpose of meeting a minor for sex. I also know from my training and experience, and as discussed further below, that child pornography offenders often store their collections on either or both a laptop and external storage media like the SD card described above.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

13. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

14. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

15. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices

were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the

computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses electronic devices to commit child pornography offenses, such devices will generally serve both as an instrumentality for committing the crime and a storage medium for evidence of the crime. They are an instrumentality of the crime because they are used as a means of committing the offense. They also are likely to be a storage medium for evidence of crime. From my training and experience, I believe that electronic devices used to commit a crime of this type may contain: data that is evidence of how the electronic devices were used; data that was sent or received; and other records that indicate the nature of the offense.

16. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

17. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

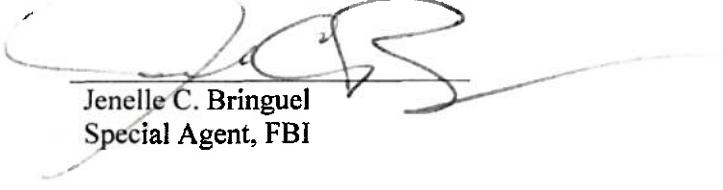
18. I respectfully submit that the information set forth in this affidavit establishes probable cause to believe that the Device contains evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) and (e) (attempted sexual exploitation of a child); 18 U.S.C. § 2252A(a)(1) (transportation of child pornography); and 18 U.S.C. § 2252A(a)(5)(b) (possession of child pornography) involving Metterhauser. Based on training, experience, and numerous interviews of subjects who admitted to having a sexual interest in children, I am aware that the following characteristics are common to individuals involved in child pornography offenses.

- a. Individuals who possess, transport, distribute, and create child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have while viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity.
- b. Individuals who possess, transport, distribute, and create child pornography may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, videos, and drawings. These individuals often maintain this material for sexual arousal and gratification. Further, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts.
- c. Individuals who possess, transport, distribute, and create child pornography often begin and build their child pornography collections by accessing the Internet and trading files with like-minded individuals on social media applications.
- d. Individuals who possess, transport, distribute, and create child pornography often maintain child pornography files on electronic devices stored in locations they deem to be relatively secure, like residences and cars. Collections are often maintained for years.

e. Individuals who possess, transport, distribute, and create child pornography often correspond with other like-minded people to share information and material, often keep records of those interactions, and have records of names, email addresses, phone numbers, and online identifiers of the people they have interacted with regarding their shared interest in child pornography.

CONCLUSION

19. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.


Jenelle C. Bringuel
Special Agent, FBI

I, the Honorable Daniel J. Stewart, United States Magistrate Judge, hereby acknowledge that this affidavit was attested to by the affiant by telephone on January 23, 2023, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

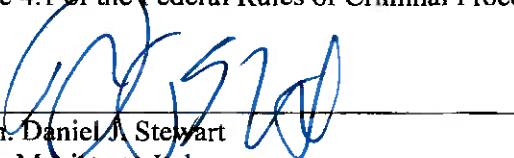

Hon. Daniel J. Stewart
U.S. Magistrate Judge

Exhibit 1

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

UNITED STATES OF AMERICA

v.

TREVOR G. METTERHAUSER,

Defendant.

)

)

)

)

)

)

Case No. 1:23-mj-00023-DJS

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of January 12, 2023 in the county of Albany in the Northern District of New York, and elsewhere the defendant violated:

Code Section
18 U.S.C. § 2251(a) and (e)

Offense Description
Attempted production of child pornography

This criminal complaint is based on these facts:

See Attached Affidavit

Continued on the attached sheet.

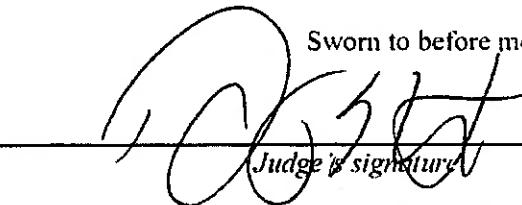


Complainant's signature

Jenelle C. Bringuel

Printed name and title

Sworn to before me:



Judge's signature

Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

Date: January 12, 2023

City and State: Albany, NY

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Jenelle Corrine Bringuel, being first duly sworn, depose and state as follows:

1. I make this affidavit in support of a criminal complaint charging Trevor Metterhauser with attempted production of child pornography, in violation of 18 U.S.C. § 2251(a) and (e).
2. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation ("FBI"). I have been so employed since 2012. While employed by the FBI, I have investigated federal criminal violations related to child sexual exploitation and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.
3. The statements in this affidavit are based upon my investigation, information provided to me by other members of law enforcement and witnesses, and on my training and experience. Because this affidavit is submitted for the limited purpose of securing a criminal complaint, I have not included all facts known to me about this investigation. Rather, I have set forth facts to establish probable cause to charge Trevor Metterhauser with attempted production of child pornography, in violation of 18 U.S.C. § 2251(a) and (e).
4. Over the past several days FBI Online Covert Employees and Task Force Officers have been communicating using a social media messaging application ("App A") with individuals operating within App A "rooms" dedicated to trading child pornography files.
5. One of those users, now identified as Metterhauser as discussed further below, has distributed in App A "rooms" files depicting the sexual exploitation of children.

6. The FBI engaged Metterhauser in a direct message conversation on a separate social media messaging application ("App B"), with an undercover investigator posing as the father of a 10-year-old deaf child available for sexual activity. During the exchange on App B, Metterhauser sent the undercover investigator child pornography files, including the following two files:

- a. an approximately 15-second video depicting a prepubescent female child nude from the waist down with her genitals displayed in a lewd and lascivious fashion while urinating; and
- b. an approximately 1 minute and 4 second video depicting a prepubescent female standing on a bed initially clothed, removing her pants, laying on her back naked, moving toward the camera, and spreading her legs to expose her vagina in a lewd and lascivious manner.

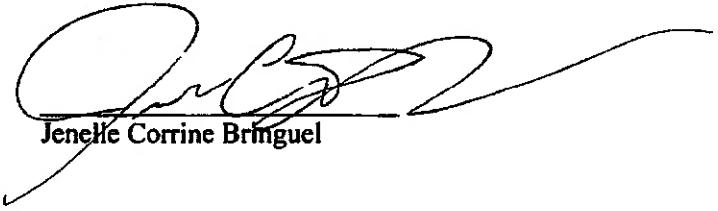
7. During the chat with the undercover investigator, Metterhauser said that, on January 12, 2023, he was going to travel from his home in Pennsylvania to the Albany, NY area to meet the child for sexual intercourse and oral sex, record that activity on a video camera that he would bring, and then sell the recording on the dark web. Metterhauser also said that he would bring a mask or paint to cover the child's face, make sure that his face was not visible in the recording, cover the windows with sheets, and bring sex toys and child pornography with him. The plan was to meet at an Albany-area fast food restaurant in the late morning and then proceed to the "father's" house so Metterhauser could have sex with the child and video record it.

8. At or around 11:00 a.m. on January 12, 2023, Metterhauser arrived at the agreed upon location. After being approached by law enforcement and being advised of his *Miranda* rights, he consented to have his car and phones searched and agreed to speak with investigators.

Metterhauser admitted, among other things, that he sent child pornography to the undercover investigator, was planning to have sex with the child, record it with his camera, and sell the recording on the dark web. He brought a video-camera, electronic storage devices that he said contained child pornography files, face paint for the child, and sex toys, all as planned and discussed in the communications. He also said that his cell phone contained child pornography files.

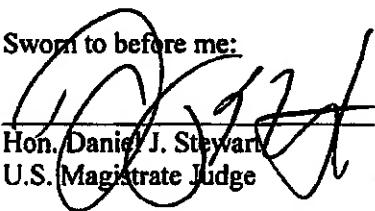
9. He further admitted to creating child pornography with a 2-year-old victim in the State of Texas in December 2022, including Metterhauser putting a lubrication device in the child's anus. He also admitted to coming to the Ithaca, NY area in the fall of 2022 and recording a female toddler whose vaginal area was exposed and being touched by another adult male. He said that the same child was drugged and that the other man recorded himself rubbing his penis on her feet and buttocks and sent Metterhauser the video files depicting that conduct.

10. Metterhauser is a registered sex offender in Pennsylvania. According to his criminal history report, he has a 2011 conviction in that State for Sexual Abuse of Children.



Jenelle Corrine Bringuel

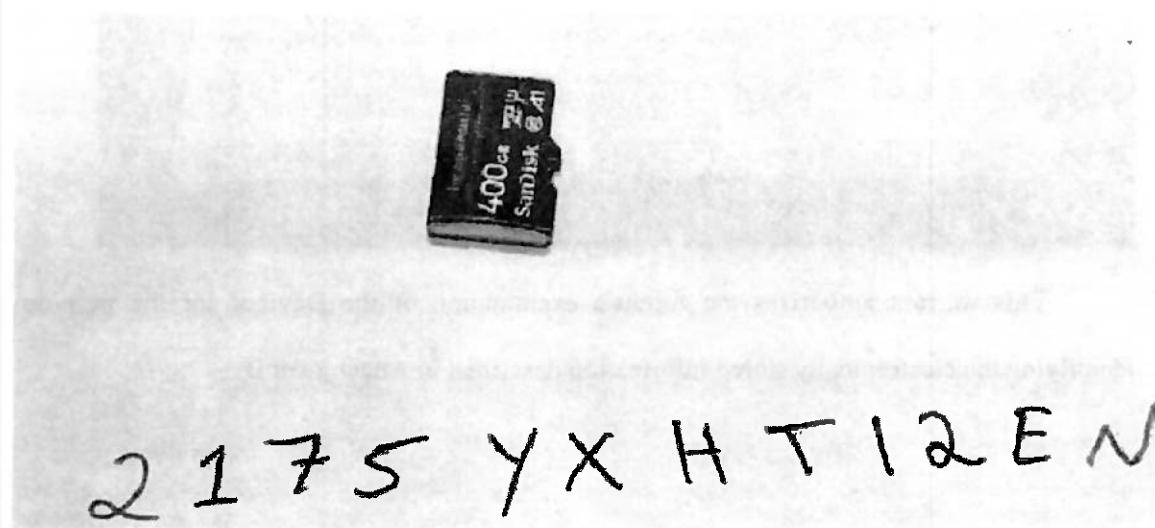
Sworn to before me:



Hon. Daniel J. Stewart
U.S. Magistrate Judge

ATTACHMENT A

The property to be searched is (1) a Microsoft 256 GB laptop, number 055196290353; and (2) a SanDisk 400 GB micro-SD card, serial number 2175YXHT12EN, which was inserted into the laptop. (Hereinafter the laptop and SD card are referred to as the "Devices.") The Devices are currently located at FBI Albany, 200 McCarty Ave, Albany NY 12209. The Devices are depicted below:





This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 2251(a) and (e) (sexual exploitation of a child, conspiracy to sexually exploit a child, and attempted sexual exploitation of a child); 18 U.S.C. § 2252A(a)(1) (transportation of child pornography); 18 U.S.C. § 2252A(a)(2)(A) (distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(b) (possession of child pornography) and involve Metterhauser, including:
 - a. Records concerning the use or attempted use of a child to create a visual depiction of sexually explicit conduct and of a conspiracy to sexual exploit a child, or the transportation, distribution, and/or possession of any visual depiction of a child engaged in sexually explicit conduct, and evidence of how any such depiction(s) were created, distributed, transported, or possessed, including evidence of what device(s) were used to create, distribute, transport, or possess the visual depiction(s), who created them or conspired in their creation.
 - b. Any visual depictions of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any visual depictions that might not meet the definition in the foregoing section but that might be considered child erotica.
 - c. Records evidencing intent, knowledge, and/or plan to create a visual depiction of a minor engaged in sexually explicit conduct or to attempt or conspire to do so, and to distribute, transport, or possess such a depiction, including evidence of an absence of any malicious software or the presence of any cleaning or data wiping or scrubbing software on the Device.
 - d. Records evidencing a sexual interest in children and/or child sexual abuse material, including an interest in visual depictions of child sexual abuse, or participation in chatrooms, social media groups, or private communications concerning the sexual abuse of children or child sexual abuse material.

e. Records of any passwords, passcodes, electronic keys, encryption/decryption codes/keys, or any other electronic record for the purpose of using such record to gain access to all or part of the data on the Device.

f. any information recording Metterhauser's schedule or travel from Pennsylvania to New York in November 2022 and January 2023 and from Pennsylvania to Texas in December 2022, including evidence of who he met or interacted with during any such travel.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records of Internet Protocol addresses used;

4. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.